THE DEPARTMENT OF HUMAN SERVICES

OFFICE OF TECHNOLOGY

LAN Support Business Plan

Last Revision: June 12, 2002

Vision: *To be a model service organization*.

Mission: *Employee; Customer; Technology*. (For detail, refer to the Product Support Mission Statement)

1 General Information

This Business Plan is available on the Office of Technology web page at WWW.HSOT.STATE.UT.US under the Policies and procedures section. This plan outlines the LAN Support Services available for all DHS facilities and non-DHS facilities supported by DHS. In general, LAN Support Services include the technical administration of the local area networks and related technology, and customer assistance with supported software applications, communication systems, and desktop hardware.

2 Services Provided

2.1 Network Operations and Administration –

? network installation, technical support, and problem resolution.
? operating system and related software installation, administration, support, and maintenance.
? performance tuning.
? Application software installation, administration, support, and maintenance.
? maintenance of customer billable device inventories.
? network topology installation, administration, support, and maintenance.
? data integrity (backup).
? network and user security.
? research and development of new or enhanced products.
? establishment of network technical standards required for efficient and consistent operation statewide.

2.2 Technical Support Services –

? customer assistance, and problem resolution.
? installation of Department standard desktop hardware and software (equipment repairs are coordinated with the applicable vendor).
? basic assistance in the use of department standard hardware and software.

2.3 Customer Consultation and Purchasing –

? consult with customers to recommend technology that is consistent with State and Department standards, and trends within the industry.

2.4 LAN and Mainframe Access –

? access forms are required for access to the LAN network or the mainframe system. Access forms are available at the receptionist desk on the first floor of the Administration Building, from OT Security, or from the Office of Technology web page at WWW.HSOT.STATE.UT.US under the support section. The policy statement on the back of the form must be reviewed and signed.

2.5 Help Desk –

? Product Support has entered into a contract with ITS to provide the first level of support for all computer, network, and phone problems. The ITS Help Desk will create a trouble ticket for every call, try to resolve the problem, and if the problem can not be resolved, the call will be dispatched to the appropriate ITS group or to the DHS Service Center.

? *OPERATIONAL POLICIES:*

The ITS Help Desk is available 24 hours a day, 7 days a week, 365 days a year. However, the DHS Service Center is available from 7 A.M. to 5 P.M., Monday thru Friday. Any calls dispatched from ITS outside of those hours, will be addressed by the DHS Service Center on the next business day.

1) ITS Help Desk
Place a call to the ITS Help Desk if you have a problem not directly related to the SAFE or ORSIS programs.

Local # -	**538-3440**
Long Distance # -	**(800)678-3440**
Online	**Http://ITS.Utah.Gov/services/support/helpdesk.htm**

2) SAFE Help Desk
Place a call to the SAFE Help Desk for problems directly related to the SAFE system.

Local # -	**538-4141**
Long Distance # -	**(801)538-4141**

3) ORSIS Help Desk
Place a call to the ORSIS Help Desk for problems directly related to the ORSIS system.

Local # -	**536-8900**
Long Distance # -	**(801)536-8900**

All calls to the ITS Help Desk will be handled in the following manner:

1) When a call is placed, the ITS Help Desk will create a trouble ticket. The caller will be required to provide the following information:

NAME	yourself or the person having the problem
PHONE NUMBER	
DEPARTMENT	
DESCRIPTION OF PROBLEM	

2) After the call has been logged into the computer, you will be given a reference number. Please write this number down and keep it handy in case you need more information about your request.

3) A severity level, or degree of seriousness, will then be associated with the problem. This identifies the urgency of the call. The severity level will be set as accurately as possible based on the following considerations:

The number of people being affected.
The importance of the function out of service
The risk to employees and/or citizens
The organization experiencing the problem, and
The long-term effects the problem could cause

The severity levels, and response times for each level, are defined as follows:

High/Urgent - response time of 30 minutes
Critical service down or complete system failure affecting a large number of people.

Medium - response time of 1 hour
Adjunct/auxiliary system failure, multiple or critical customers out of service, many inconvenienced but still able to work, unrecoverable loss of data and/or revenue.

Low - response time of 2 hours
All other problems.

4) The ITS Help Desk will try to resolve the problem immediately. If the problem can't be resolved it will be dispatched to the DHS Service Center.

5) If the call is dispatched to the DHS Service Center, trouble tickets will be addressed according to FIRST IN FIRST OUT. At that time, if the call can't be resolved within **15 minutes,** the call is dispatched to the appropriate DHS group.
NOTE: A problem must have a trouble ticket to be addressed.

6) If the call is dispatched by the DHS Service Center to one of the Region Support teams, it will be addressed according to Severity Level and/or FIFO. If needed, they will schedule an on-site visit.
NOTE: Site visits will be directly related to trouble tickets and the need for on-site resolution.

7) If the call is dispatched by the DHS Service Center to the Control Center, trouble tickets will be addressed according to Severity Level.

8) Upon resolution, either by the ITS Help Desk or appropriate ITS group, or by the DHS Service Center or appropriate DHS group, the trouble ticket will be set to **RESOLVED** status and automatically closed in 15 days**.** Except in extraordinary situations, a problem will be closed in 15 days from the time it was set to a status of **RESOLVED** unless otherwise specified by the customer.

Escalation Procedures:

Escalation, Option 1:
Call the ITS Help Desk and ask for your problem to be escalated. The management of the organization to which your problem is assigned will be notified. They will respond to your request and contact you to discuss the situation.

Escalation, Option 2:
Call the ITS Help Desk and ask to speak to the Duty Manager. If on site, you will be connected to the Duty Manager immediately. Otherwise, the Duty Manager will be paged and will promptly contact you.

Feedback:
Your satisfaction with the service provided, from the moment you place a call to the moment of resolution, is important to all of us. You will be surveyed periodically to help all of us maintain and/or improve the level of service being provided.

2.6 Telecommuting (remote access) –

? Telecommuting (remote access) is currently available in Ogden, Provo, and Salt Lake. Several options are available, depending on the level of use required. Refer to the options listed below to select the appropriate solution based on your access requirements and secondary office location.

? Telecommuting Summary

To telecommute, an employee must complete a telecommuting contract. Upon completion and approval of the telecommuting contract contact the following:

If you live in the Salt Lake local calling area, call the Help Desk at 538-3440.

If you live in the Ogden local calling area, call ITS staff at 626-3770.

If you live in the Provo local calling area, call ITS staff at 374-7870.

Approximate costs for telecommuting are summarized below:

Internet Service Provider:

This option is the customer's responsibility. The State does not have a contract with an ISP.

Dialup Remote Access (Citrix):

Direct Dial-In ICA:

? Local calling area.
? Private providers.
? Individuals needing access to Department standard applications only.
? Charges:

Full-time telecommuter:
$25.00 per month for an additional phone line (optional)
$67.50 per month for setup and support
$31.00 per month for Wide Area Network

Part-time telecommuter:
$25.00 per month for an additional phone line (optional)

ICA over NetWare Connect:

? Local calling area with need for IPX.
? Individuals who can demonstrate a need for an application not available on Citrix.
? Charges:

Full-time telecommuter:
$25.00 per month for an additional phone line (optional)
$67.50 per month for setup and support
$31.00 per month for Wide Area Network

Part-time telecommuter:
$25.00 per month for an additional phone line (optional)

Dialup Remote Access:

Ogden/Provo area:

Full-time/Part-time telecommuter:
$25.00 per month for an additional phone line (optional)
$50.00 per hour for setup and support
$31.00 per month for local dialup resources

ISDN Remote Access:

Salt Lake area:

Full-time telecommuter:
$120.00 per month
$1500.00 installation charge (varies)
$67.50 per month for setup and support

Part-time telecommuter:
$120.00 per month
$1500.00 installation charge (varies)

Ogden/Provo area:

Full-time/Part-time telecommuter:
$120.00 per month
$1500.00 installation charge (varies)
$50.00 per hour for setup and support

NOTE: The above costs are for DHS staff housed in DHS supported offices.

2.7 Training-

? training is provided on all standard applications (refer to section 7). The training is $25.00 per half-day class, per employee. A full day class is $50.00 per class, per employee. One on one training is available at $50.00 per hour. Contact Janice DeVore at 538-4050 for additional information.

2.8 After Hours Support-

? After hours assistance is provided for emergency situations outside of the normal work hours of 7am – 5pm, Monday through Friday.

? After hours assistance is provided at the rate of $50/hr.

? After hours assistance is requested by placing a ticket to the ITS help desk:

Local # -	**538-3440**
Long Distance # -	**(800) 678-3440**

? Tickets requesting after hours support will be dispatched to the Unix staff on call. The Unix staff will determine the cause of the problem and make contact with staff based on a call list.

? If contact cannot be made with staff on the call list, the problem will be dealt with promptly on the following, regular work day.

3 Service Commitments and Response Time (support commitments and response times are generally accepted by ITS and DWS supported sites as well).

3.1 Production Problems - network problems affecting multiple users take priority and are responded to immediately. Restoration of a down server may take up to 48 hours, depending on type of failure. Agencies may conduct mission critical functions at a nearby DHS office location, until restoration can be completed.

3.2 Problem Resolution - problem resolution and user access related support requests are to be completed within 2 working days. In some instances travel, hardware failure, or the need for further research may make 2-day resolution improbable. Refer to section 4.4 for the service escalation process.

3.3 Customer Requests - installation of new hardware, software, telecommuting setup?, equipment moves, changes to data wiring requests, etc. are to be completed within 5 working days.

3.4 Training Room Setup Requests - installation of hardware or software, equipment moves, data wiring changes, etc. are to be submitted to the ITS Help Desk a minimum of 5 days in advance to allow time for completion.

3.5 Agency Wide Initiatives - an acceptable time frame will be negotiated with the customer agency and the time frame will be determined by 1) customer's priority, 2) level of effort involved, and 3) current workload.

3.6 Supported Technologies - services are provided for all department standard hardware and software products (see section 7). Customers who maintain additional commercial software on their workstations i.e., local disk drives, or other writeable media, may do so if the software supports a government related function, and is in compliance with all licensing and copyright laws. The employee or agency must retain documentation of ownership and is responsible to purchase the software. OT staff will not support these products. OT staff are expected to fully support the hardware standards listed in this document. If customers purchase additional hardware products they will not be supported on the DHS LAN networks or by the OT staff.

3.7 If customers have a specific technology need that can not be reasonably satisfied with current supported network resources (software or hardware) and would like the product to be on the Standards list, contact Debbra Naegle at 538-4638 for additional information regarding the process for changing or adding supported technology standards.

3.8 Agency specific software will be approved as an agency standard if the product meets the criteria for an agency standard, if the agency agrees with the terms of the Agency Software Standard policy, and if the agency follows the approval process. A request for consultation must be placed with the ITS Help Desk.

3.9 All standard software applications supported on DHS networks will be maintained for the current release. There will be a transition period from the previous release to the current release, and that transition period will be determined based on the individual product and the impact to DHS customers. The transition period will be approved by the OT Director. Customers are encouraged to migrate to the new release as quickly as possible.

4 Service Areas and Coverage

4.1 DHS Supported Sites (120 N. 200 W. SLC)

Product Support is composed of four units:

Service Center
Supervisor: Fred Schmidt
Hours of Operation: 7A.M. to 5 P.M., Monday thru Friday
- The Service Center will address trouble tickets dispatched to them by the ITS Help Desk. The goal is to resolve the ticket. If the ticket is dispatched from the Service Center, it will be dispatched to the appropriate group as outlined below.

Region 1 Support
Supervisor: Peter Freeman (538-4579)
Hours of Operation: 7A.M. to 4 P.M., Monday thru Friday
- The Region 1 Support team will provide on-site support for the Northern Region sites.
DHS Administration Building Hours of Operation: 7 A.M. to 5 P.M., Monday thru Friday
- The Region 1 Support team will provide on-site support for the DHS Administration Building.

Region 2 Support
Supervisor: Fred Schmidt (550-8322)
Hours of Operation: 7A.M. to 4 P.M, Monday thru Friday
- The Region 2 Support team will provide on-site support for all sites in Central Region and all sites south.

Control Center
Supervisor: Greg Casey (538-4637)
Hours of Operation: 7A.M. to 4 P.M, Monday thru Friday
- The Control Center provides support for all of the global functions within DHS (servers, GroupWise, etc.). They also provide technical support to the Region Support teams.
After hours support for Unix is available by paging Greg Taylor at 580-1603 or Ted Pardike at 580-1826.

4.2 Ogden and Provo Regional Centers (ORC and PRC)

Service is provided by the Division of Information Technology Services (ITS). Coverage is provided from 8:00 a.m. until 5:00 P.M., Monday through Friday. For service and support in the Ogden Regional Center contact the ITS staff at 626-3770. For service and support in the Provo Regional Center contact the ITS staff at 374-7870.

4.3 DWS Supported Sites

Customers in DWS supported sites should contact their assigned LAN Administrator between the hours of 7:00 a.m. and 4:00 p.m. and the DWS Help Desk for problem resolution between 4:00 p.m. and 5:00 p.m. On call or after hours support is not provided to the regional office locations at this time.

4.4 Service Escalation Process

Escalation Procedures for DHS supported sites:

Escalation, Option 1:
Call the ITS Help Desk and ask for your problem to be escalated. The management of the organization to which your problem is assigned will be notified. They will respond to your request and contact you to discuss the situation.

Escalation, Option 2:
Call the ITS Help Desk and ask to speak to the Duty Manager. If on site, you will be connected to

the Duty Manager immediately. Otherwise, the Duty Manager will be paged and will promptly contact you.

Escalation Procedures for DWS supported sites:
In region office locations supported by Workforce Services contact Jim Matsumura at 526-9526.

Escalation Procedures for ITS supported sites:
For the Ogden Regional Center contact Wanda Wintle at 626-3771 and for the Provo Regional Center contact Val Danklef at 374-7870. For service issues in the Ogden and Provo Regional Center, you can also contact Russ Fairless at 538-3492.

5 LAN Support Service Rate and Other Applicable Charges

5.1 LAN Support Rate

The Department of Human Services and Workforce Services current rate is $67.50 per month per supported device as of July 1, 1999. All supported desktop devices (which includes laptops used as a desktop device or in a pool for checkout) are assessed these rates. This rate does not include server based software and hardware. Additional charges may apply for telecommuting or remote access capability. This charge is assessed quarterly. Refer to section 2.6 for an explanation of applicable charges.

Note - In the Ogden and Provo Regional Centers the LAN Support Rate is $65.00 per device. They include printers as a chargeable device.

5.2 Software Charges

Standard software applications are paid by the Office of Technology on a quarterly basis. This quarterly cost is then charged back to participating agencies based on their reported device counts. Currently this process covers all Novell, Microsoft, and Folio software products used on DHS LAN networks, or installed for employees who are telecommuting. These quarterly software charges are not included in the LAN Support Rate and average approximately $10.00 per device per month.

Note - In the Ogden and Provo Regional Centers software is included in the Lan Support Rate.

5.3 Wan Charge

A wide area network charge of $31.00 is assessed for every device connected to the WAN, by ITS on a quarterly basis.

5.4 Additional charges

A charge of $50.00/hr. may be assessed for support of some remote operations (schools), for support of some non DHS Departments/agencies (AG, Health) requiring occasional support, and for setup and support of standalone equipment.

5.5 Agency Specific Software

If customers purchase additional commercial software for use on their individual hard drives, the employees agency is responsible for the licensing costs and to maintain appropriate documentation of ownership and legal licensing of the products in use.

5.6 LAN Server Hardware Costs

Hardware costs required to support the local LAN network servers and related components are not included in the LAN support rate. These costs are supported with 50% paid by the Department Executive Director's Office and the balance paid by the agencies, based on the device count. The Ogden and Provo Regional Center LAN server hardware costs are included in their $65.00 LAN Support Rate.

SERVER REPLACEMENT CRITERIA

If device count > 50, replace every three years to take full advantage of new technology
If device count < 50, replace if:

performance issues consistently cause problems
upgrading is more costly than replacement
new technology provides benefits that justify replacement
server is five years old

5.7 LAN Desktop Hardware Costs

Hardware costs required to support the desktop are not included in the LAN support rate. These costs are paid by the agencies.

PC REPLACEMENT CRITERIA

If PC is three years old, replace
If PC is under three years old, replace if:

agency business need exists (i.e. SAFE)
technological environment dictates
upgrading is more costly than replacement

6 LAN Maintenance Policies

6.1 Retention – Every week GroupWise maintenance is performed. During maintenance all E-mail messages, inbox and outbox, older than 90 days are deleted and trash older than 30 days. If you must keep messages past 90 days you may create an Archive Folder in your personal directory, or save the item to Word.

6.2 Lost Documents - To have a document restored to the system, call the ITS Help Desk and make a request. Indicate the directory and document name to be restored.

6.3 Downtime - for the local area networks in the DHS Administration Building downtime is scheduled every Tuesday morning from 6:00 am until 7:00 am to conduct system maintenance. The third Saturday of each month is also designated as a maintenance day from 10:00 p.m. until 6:00 p.m. The State mainframe systems are down each Sunday from 6:00 a.m. until 12:00 p.m. (Noon).

Downtime, for the region office locations, is scheduled in advance with the local agency representatives and is scheduled after regular business hours, unless unavoidable.

6.4 Standard Software Applications - supported on the DHS networks will be maintained for one release with a transition period from the previous release. Customers are encouraged to migrate to the new releases as quickly as possible.

6.5 LAN Hardware Maintenance Coverage - for all DHS servers on warranty, hardware replacement is provided within 24 to 48 hours. Critical parts i.e., disks and power supplies are maintained for all DHS servers on warranty. DHS servers not on warranty, hardware maintenance coverage is provided by Telos, and replacements are made within 48 hours.

6.6 Data Integrity - is provided for all DHS servers. Backup is performed daily on a two-week rotation, weekly on a monthly rotation, and monthly on a three-year rotation.

7 Department standard software applications

The following is a list and brief description of the current Department standards for supported software applications and application suites.

?

? LAN Workplace Pro Current Version: 5.2

This product offers a variety of IP based services i.e., TN 3270 IP emulation, Rapid Filer, Telenet, etc.

?

? GroupWise Current Version: 5.5e

Office automation "E-MAIL" tool that allows correspondence with other E-mail users, maintain electronic calendars, and to schedule appointments with others or manage resources. This product also allows you to manage your daily tasks, notes, and phone messages or those of others.

?

? Microsoft Office Professional (suite) Current Version: 2000

Containing the following Applications:

Access: This program is a database development and reporting tool. This is an advanced product targeted for user level development to maintain, report and manage information.

Excel: This product is a high-end graphical interface spreadsheet with features such as; spreadsheet publishing (graphics), three dimensional worksheets and charts, database access, and other advanced features.

PowerPoint: High-end presentation graphics with advanced charting, draw, and graphics capabilities. This product is used to present charted data, graphics, overheads, and slide show presentations. Video and sound is available for multimedia presentations.

Word: Integrated high-end word processing and document publishing application that includes powerful graphics capability and the basics in spreadsheeting and database functionality.

? Microsoft Office Standard (suite) Current Version: 2000

Containing the following Applications:

Excel: This product is a high-end graphical interface spreadsheet with features such as; spreadsheet publishing (graphics), three dimensional worksheets and charts, database access, and other advanced features.

PowerPoint: High-end presentation graphics with advanced charting, draw, and graphics capabilities. This product is used to present charted data, graphics, overheads, and slide show presentations. Video and sound is available for multimedia presentations.

Word: Integrated high-end word processing and document publishing application that includes powerful graphics capability and the basics in spreadsheeting and database functionality.

? Informs Current Version: 4.3

An application used to fill out forms and surveys, and develop electronic forms. This product also allows you to collect and maintain the information in various database products. It also is a tool for producing printed forms. The product has two parts, Filler and Developer. All users are given the Filler portion of the product. Developer setup must be requested.

? Netscape Current Version: 4.08

A browser used to access the internet. This tool allows access to the Internet; i.e., World Wide Web and FTP servers.

X Internet Explorer Current Version: 5.01
A browser used to access the internet. This tool allows access to the Internet; i.e., World Wide Web and FTP servers.

X Microsoft Windows Current Version: 95/2000
This product is the desktop operating system and interface to the applications.

8 Special software applications

The following products are supported by the Department. However, they must be specified separately on the Departments Security Access Form, or requested by the customer. Some of the applications listed will require the purchase of a license.

? SPSS
Statistical data analysis tool.

? Microsoft Project
Automated project management tool - available on a per request basis.

? Finet
A graphical interface to the FINET system on the Mainframe.

? OLGL
The financial On Line General Ledger System.

? HR Enterprise
The human resource tool.

? Visio
A flow chart software tool.

? SAFE
Child and Family Services tool.

9 Department hardware standards

The desktop and laptop hardware standard is as follows:

Minimum purchase:

- 1Gig Pentium processor
- 32X CDROM
- Sound card
- 20GB hard drive
- 128 or 256 MB memory
- Windows 2000/FAT 32
- 10/100 Ethernet Card – Choices Include:
  - 3Com
  - Intel
- 17" monitor

Desktop/Laptop recommended vendors:

GATEWAY
DELL
COMPAQ (DESKTOP ONLY)
TOSHIBA (LAPTOP ONLY)

Printers:
HP
JetDirect Card (IP capable)
Standard sheet feeder/tray options

PDA's:
Windows CE device

10 Network Management of Devices being attached to the Human Services Network

Introduction

Due to an increase in a variety of devices being attached to the Human Services portion of the State of Utah Wide Area Network, the Office of Technology recognizes the need to review and control those devices in a coherant and managed process. It is the contention of the Office of Technology Security Group that any device that is being attached to the network must reviewed by the various support groups within OT to ensure that functionality, as well as information security can be achieved. In the past, there has not been an effort to control the various agency actions as they pertain to obtaining new devices that are to be integrated into the network. With technology advances, more and more of these devices are becoming network ready. That is the device has a network interface card (NIC) and a fully functional operating system installed. This in turn allows the device to be integrated into the network without any regard to proper management, but more importantly without regard to proper security review.

Definitions

Device: A device can be defined as any piece of equipment or hardware that can be attached or integrated into the network. This would include any device that has an installed network interface card (NIC) or can be attached to a device that would act as a network interface device or a functional operating system. Essentially it means any device that can be visible through an operating system to a user attached to the network.
Network: The network can be defined as that area of the State of Utah Wide Area Network that is administered by the Office of Technology of the Department of Human Services.
Installed or Attached: The process where by a device or a piece of equipment is either physically or logically connected to the network.

Device and Equipment Procedure

? The Office of Technology will review any device that can be attached to the network in order to provide optimum levels of support. The device will also be reviewed to ensure that proper security measures are in place as they apply to the network, as well as the device.

? A Service Request ticket must be submitted to the Office of Technology regarding intent to install a device to the network. The Service Request must contain specifications of the device as to whether it is a network capable device or not. Location of the where the device will be installed, whether an outside vendor will be involved in the installation.

? A review of the device by network management and the security group will determine the viability of the device in a network environment. Once the review has been completed, Office of Technology will either give permission to proceed, or will deny permission or recommend another device.

Conclusion

The Office of Technology recognizes that each agency has unique needs in order for that agency to provide services to its clients. It is to the benefit of each agency to recognize the need for standardization of equipment. This in turn allows the Office of Technology the ability to provide the best support possible with an established number of device types.

11 Office Of Technology Information Security Procedures and Practices

Background

Access to the information resource infrastructure within the Department of Human Service require that each and every user accept responsibility to protect the rights of the employees and the clients of the Department of Human Service. The conditions and procedures for requesting access are outlined in the Policy on Acceptable Use of Information Technology Resources of the Department of Human Services. Any person who requires access to any Information Technology Resources must submit the appropriate request form to gain access. These access requests are applicable to all platforms, operating systems, devices, and applications, which are under the administrative control of the Office of Technology of the Department of Human Services. Any change in status, termination, requests for additional access, will require that the appropriate forms be submitted to implement the requested change. This is applicable to additional software or applications, changes in locations or agency, changes in allowed space, or time restrictions, or any other change that may impact the operation of Information Technology Resources.

Security Procedures and Practices

Purpose

Information security is essential for the effective and efficient operation of the network and for the provision of network services. Security is the responsibility of all members of the Department, including users of the network, local technical staff, and network support staff. Any person who requires access to the network shall submit documentation to the appropriate Security Group or Help Desk as it applies to each organization. The documentation will indicate the level of access required to carry out their job function; documentation will be signed by both, the user and supervisor, and or the manager as applicable. Any request form where one or both of the required signatures is not present, that form will be returned to the point of origin for correction. Access level will be granted based on legitimate business need in order to fulfill the job function of the employee. These steps are outlined in the Policy on Appropriate Use of Information Technology Resources.

It also must be recognized that the people who utilize the services of the Department of Human Services are the key element to our organization. The information that they entrust to us must be protected and safeguarded. It is critical that they have confidence in our ability to protect them from indiscriminate disclosure. This is a crucial element in the overall strategy as it applies to Information Security.

General Guidelines

Security Procedures and practices are made up of various elements that protect the information technology resources of the Department. Those elements are access control, accountability, separation of duties, and other procedures and practices that are used to maintain security integrity. The following information is a basic explanation of each element as it applies to information security.

Access Control is the practice of allowing and limiting the amount of access that is available to any person as it applies to Information Technology. In order to access any IT resource a person must submit proper documentation in order to access that resource. The documentation will contain elements that provide information as to the level of availability of the resource that is being requested. It will also contain a counter signature of the manager or supervisor of the person who is requesting the access.

Due to the large number of different job functions, the supervisor of the employee that is requesting access must take responsibility for the level of access that is being requested. The supervisor or manager is the person who is most familiar with the job function of the employee and should be the best judge of what level of access is best suited for employee.

Accountability refers to the ability to identify access to a particular user. For example, each user for any of the UNIX platforms receives a unique ID. That unique ID is used even if the user uses su to assume a level of access other than their own. The SULOG provides that method of accountability. That is why it is important that any person who receives an ID to access the system, not share it with anyone and always use that ID to login with. It is critical that for the most part, Department employees will not use system or application ID's for the initial logon to the system, no matter the platform or operating system.

Separation of duties deals with the need for separation of areas of access. For example, it is an industry standard to allow developers and programmers extensive access to any development or testing area, as long as there is no interaction with a production environment. If there is interaction, such as moving code or programs from test to production, that process will be strictly controlled so that a third party will move the code to production. In the Department of Human Services, programmers submit a migration form to the Security in order to have completed code and programs moved from test to production. This practice extends to the average user level as well. Standard business practices call for separation of fiscal duties so that one party may not control the entire process of any fiscal transaction. For example, the Department of Human Services makes payments to certain persons or organizations for services rendered to clients of the Department. The term used for those parties is called a provider. Separation of duties must exist between those employees that have the ability to create a provider and those employees who then make payments for those services rendered by that provider.

It also must be recognized the Information Security is a balancing act; business function vs. information security. Too much security and functionality is lost. Too much functionality risks the potential for disclosure and as well as possible disruption of the system. This in turn lead to loss of confidence by the user community as well as clients employing the services of the Department.

Components

User accounts will be set up to correspond to an individual rather than a location or a function in order to provide accountability. The use of generic accounts will be strictly limited. If a generic account is used the account will be station restricted in order to provide some level of security. Exceptions will be made for technical accounts that provide mainframe print services or is of a technical nature that provides functionality for the system. In some cases applications will need user accounts established in order to provide functionality. This is present on the UNIX platforms where accounts exist for example, for the Sybase Administrative account, or to the Control M account on the mainframe which is used for job scheduling and automated job submission. Exceptions made need to be made in order for those accounts to function properly. An exception may be that the file access may be of a more extensive nature in order to perform certain functions.

The standard for all user accounts, this includes all networks, operating systems, and devices, including the State of Utah Mainframe System, will be as follows:

1. Password length will be six characters.
2. Passwords will be changed at a maximum of every ninety days. A shorter password change period may be set at the request of the owner of the account. A password may be changed at anytime by the owner of an account if in the event a security issue is indicated.
3. Accounts will have six grace logons before the account is locked.
4. User account home directories unless otherwise indicated shall be limited to 20 MB of space.
5. Intruder detection will be set on all containers at six attempts in a thirty-minute period and the account will be locked for 999 days. The Department of Human Services Security Administrators will only unlock accounts once a satisfactory response is received regarding the failed attempts.
6. Accounts will be time restricted for hours of operation from 12:00 AM to 05:00 AM unless a legitimate business need is indicated for extended use.
7. Concurrent connections will be three, unless a legitimate business need is indicated. At no time will any account have unlimited connections. All accounts must have a finite number of connections; this also includes technical staff.
8. Users with password access to systems or services are responsible for maintaining the security of their password(s). Users will not share, post or display logon ID's and passwords.
9. Accounts for any user that is terminated or leaves employment with the Department of Human Service or any other institution that access Department of Human Services Information Technology Resources shall submit exit documentation to the applicable agency for final disposition. _Documentation will be submitted by the supervisor of that employee indicating that this employee has left employment and their accounts and files need to be disabled for a ten-day period and subsequently deleted after that ten-day period. The Exit Interview form can be obtained from the Department of Human Services Security Group or is available online at http://www.hsot.state.ut.us/forms/forms.htm.
10. All servers shall be kept in a secure location, through either a secure room or secure cabinet in order to safeguard this equipment. All servers will use the console keyboard lock out when not being accessed by technical staff. All measures will be employed to insure that casual contact by non-technical staff will not occur.
11. In the event an exception is requested: time restriction, concurrent connection, space limitation, etc… the Department of Human Services Network Access form must be submitted with the appropriate signatures. Under the section, marked Special Applications shall contain the information related to the exception. The supervisor of the person

requesting the exception must sign and date the form. This form can be obtained from the Department of Human Services Security Group or online at http://www.hsot.state.ut.us/forms/forms.htm. Due to variations that exist at other agencies that are under the administrative control of the Department of Human Services, a general agency exception can be granted via a memo requesting the exception with the signature of the Office of Technology director or the equivalent position that exists at that level. This memo shall be filed with the Department of Human Services Security Group to be kept on file for the duration of the exception.

12. In the event expanded access or additional software is needed; the DHS Network Access form must be submitted with the correct information and signatures.

13. In the event of suspicious activity, contact will be made with Department of Human Services Security group to report the activity and any details that may be relevant to any areas of concern as it relates to the activity in question

14. Any person or organization that is not an entity of the State of Utah, that is an agency, department, or other such organization, or individual that is not an employee of state government shall not be granted access, unless the Director of Human Services or their chosen deputy, requests access in writing authorizing such access. This access shall also be registered with the Bureau of Internal Review and Audit for the duration of the access. Unlimited access will not be granted to any non-state agency or individual, specific restrictions will exist as to length of account, method of access, and specific restrictions on access depending on platform and application. This access will be reviewed with the Office of Technology Security Group and Bureau of Internal Review and Audit to ensure proper restrictions and controls are enforced. Periodic review of the access that is granted, will occur with the requesting agency, Office of Technology Security Group, and the Bureau of Internal Review and Audit to ensure compliance.

15. In the event a request is received regarding a violation of the Departments Appropriate Use of Information Technology Resources Policy or there is a violation of any existing State of Utah Acceptable Use or Security Policies and the need for an investigation is deemed as necessary. The Investigating Authority will provide to the OT Security Group a written document from the Director of Human Services or their designee, indicating that access will be granted in order to conduct the investigation. Access will only be granted once that document is received. This document will be kept on file in the OT Security Group archives. A copy can be provided to the Investigating Authority upon request.

16. In accordance with the directive from the Chief Information Officer of the State of Utah's Policy for Limiting Access to Inappropriate Internet Sites, content filtering will be used to limit access to inappropriate sites. The directive can be found at http://www.cio.state.ut.us/399/contentfilltering.htm. Due to the diverse nature of agencies that are under the Department of Human Services and due to the nature of various job functions, there may be employees who may need access to sites that are deemed inappropriate according to the present policy. An employee who falls into that category shall request that their supervisor send an Email to the OT Security Group indicating that the employee listed in the Email, in order to perform their job function will need access to sites that may be deemed inappropriate according to the present policy. The Supervisor will list the nature of the sites that may be accessed in order for the employee to perform their duties. OT Security will then forward the exception to the ITS Security Group responsible for the filtering application. This document will be kept on file in the OT Security Group archives. The exception will also be registered with Human Resources Management.

17. The Office of Technology in conjunction with Human Resources Management shall review inappropriate access to the Internet and Internet Sites and Services based on the

Department of Human Services Acceptable Use of Information Technology Resources Policy as it applies to employee infractions that are under review.